Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- Hva er kryptering?
- Hva kan du kryptere?
- Gjør det riktig

Kryptering

Hva er kryptering?

Du har sikkert hørt folk bruke uttrykket "kryptering", og hørt dem snakke om hvordan du burde bruke det for å beskytte deg selv og din informasjon. Men kryptering kan være forvirrende, og det er viktig å kjenne til begrensningene. I dette nyhetsbrevet vil vi på en enkel måte forklare hva kryptering er, hvordan det beskytter deg, og hvordan det skal implementeres riktig.

Gjesteredaktør

Francesca Bosco (@francibosco) er forsker og prosjektoffiser, og leder prosjekter relatert til cyberkriminalitet, cybersikkerhet, og misbruk av teknologi. Hun jobber ved United Nations Interregional Crime and Justice Research Institute (UNICRI), og hun var med å starte senteret for teknologi og lov (Tech and Law Center).

Vi har utrolig mye sensitiv informasjon lagret på diverse enheter, som personlige dokumenter, bilder, og e-poster. Om en av enhetene dine blir stjålet, kan tyven få tilgang til all denne sensitive informasjonen. I tillegg kan det være du gjennomfører sensitive handlinger på nettet, som bruk av nettbank, eller netthandel. Om noen overvåker disse handlingene kan de stjele informasjon, som kontodetaljer eller bankkortnumre. I slike tilfeller beskytter kryptering deg, slik at uautoriserte ikke får tilgang til informasjonen din.

Kryptering har eksistert i tusenvis av år. I dag er kryptering mye mer sofistikert enn før, men poenget er det samme – å sende en hemmelig beskjed fra et sted til et annet uten at uautoriserte skal kunne lese den. Ukryptert informasjon kalles for klartekst. Det vil si at alle enkelt kan få tilgang til, og lese informasjonen. Kryptering gjør om informasjonen til ikke-lesbar chiffertekst. Dagens kryptering benytter komplekse matematiske operasjoner og en unik nøkkel for å konvertere informasjon til chiffertekst. Nøkkelen er det som låser og låser opp informasjonen din, i de fleste tilfeller er nøkkelen et passord.

Hva kan du kryptere?

Helt generelt er det to typer data som kan krypteres. Stillestående data (som dokumenter på mobiltelefonen din), og data i bevegelse (som når du mottar en e-post eller sender melding til en venn).

Det å kryptere stillestående data er en vital del av det å beskytte informasjon dersom din datamaskin eller mobile enhet blir borte eller stjålet. Dagens enheter er ekstremt kraftfulle, og inneholder enormt mye informasjon, men det er også veldig

© SANS Institute 2016

Kryptering

enkelt å miste dem. I tillegg kan andre former for mobile medier inneholde sensitiv informasjon, for eksempel USB-minnepinner og eksterne harddisker. Fulldiskkryptering (FDE), er en mye brukt krypteringsteknikk som krypterer en hel disk i systemet ditt. Det betyr at alt på systemet automatisk blir kryptert, så du slipper å bestemme hva som skal og ikke skal krypteres. I dag kommer de feste datamaskiner med FDE, men du må kanskje skru det på manuelt. På Mac-maskiner kalles det FileVault, mens på Windows-maskiner, avhengig av versjon, kan du bruke enten Bitlocker eller Device Encryption. De fleste mobile enheter har også støtte for FDE. iOS på iPhoner og iPader skrur på FDE automatisk når et passord har blitt bestemt. Fra og med Android 6.0 (Marshmallow) krever også Google at FDE er aktivert som standard, så lenge maskinvaren møter minimumskravene.

Kryptering er til veldig god hjelp for å sikre informasjonen din, men den er ikke sterkere enn krypteringsnøkkelen.

Informasjonen er også sårbar når den blir sendt fra et sted til et annet. Dersom den ikke krypteres, kan dataene bli overvåket, endret, og snappet opp over nettet. Derfor bør du sørge for at enhver sensitiv transaksjon eller kommunikasjon over nettet er kryptert. En vanlig form for kryptering for internett-kommunikasjon er HTTPS. Når det er i bruk, er all kommunikasjon mellom nettleseren din og nettsiden kryptert. Se etter https:// i URL-en, et låsesymbol i nettleseren, eller et grønt URL-felt. Et annet eksempel er sending og mottak e-post. De fleste e-postklienter har krypteringsalternativer som du kanskje er nødt til å aktivere manuelt. Et tredje eksempel på kryptering av data i transitt, er to brukere som chatter med hverandre, for eksempel med iMessage, Wickr, Signal, WhatsApp eller Telegram. Apper som disse tilbyr ende-til-ende kryptering, som hindrer tredjeparter i å få tilgang til dataene mens de sendes fra et endepunkt til et annet. Dette betyr at kun du og personen du kommuniserer med kan lese det som sendes.

Gjør det riktig

For å være sikker på at du er beskyttet når du bruker kryptering, er det veldig viktig at du gjør det riktig.

- Krypteringen er ikke sterkere enn nøkkelen. Om noen gjetter seg frem til nøkkelen, eller får tak i den på andre måter, har de tilgang til dataene dine. Derfor er det veldig viktig at du beskytter nøkkelen din. Om du bruker et passord som nøkkel, må du sørge for at det er sterkt og unikt. Jo lenger det er, jo vanskeligere er det for en angriper

Kryptering

å gjette det, eller finne frem til det med et uttømmende søk. Ikke glem passordet ditt heller, uten nøkkelen kan du ikke dekryptere informasjonen din. Dersom du ikke klarer å huske alle passordene dine, anbefaler vi at du bruker et program eller en app for passordhåndtering.

- Krypteringen din er ikke sterkere enn sikkerheten til enheten din. Dersom enheten din er kompromittert eller har blitt infisert med skadevare, kan cyberkriminelle komme rundt krypteringen. Derfor er det veldig viktig at du også tar andre grep for å sikre enhetene dine, ta blant annet i bruk antivirus, ha sterke passord, og hold enhetene oppdatert.
- Mange apper og programmer tilbyr nå sterk kryptering for å beskytte data og kommunikasjon. Dersom appen eller programmet du bruker ikke støtter kryptering, bør du vurdere alternative apper eller programmer.

Lær mer

Abonner på det månedlige OUCH!-nyhetsbrevet om sikkerhetsbevissthet, se gjennom OUCH!-arkiver, og lær mer om SANS sine løsninger for sikkerhetsbevissthet ved å gå inn på securingthehuman.sans.org/ouch/archives.

Norsk Versjon

NorSIS arbeider for at alle skal kunne bruke internett og IKT trygt på jobb og privat. Vi er både samarbeidspartner og pådriver overfor myndigheter og bedrifter. NorSIS er et uavhengig organ som ønsker å gjøre informasjonssikkerhet til en naturlig del av hverdagen.

Ressurser

Kryptering forklart:	http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
Passordsetninger:	https://securingthehuman.sans.org/ouch/2015#april2015
Passordhåndterere:	https://securingthehuman.sans.org/ouch/2015#october2015
Hva er skadevare?:	https://securingthehuman.sans.org/ouch/2016#march2016
Slik sikrer du ditt nye nettbrett:	https://securingthehuman.sans.org/ouch/2016#january2016

OUCH! utgis av SANS Securing The Human, og er distribuert under Creative Commons BY-NC-BD 4.0 lisensen. Du står fritt til å distribuere dette nyhetsbrevet, eller bruke det i ditt eget bevissthetsprogram, så lenge du ikke gjør endringer på nyhetsbrevet. For oversettelser og mer informasjon, ta kontakt med oss på ouch@securingthehuman.org.

Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Oversatt av: NorSIS

securingthehuman.sans.org/blog /securethehuman @securethehuman securingthehuman.sans.org/gplus